

FILED BY FAX

1 James S. Notis
 2 Jennifer Sarnelli (State Bar No. 242510)
 3 Kira German
 4 **GARDY & NOTIS, LLP**
 5 501 Fifth Avenue, Suite 1408
 6 New York, NY 10017
 7 Tel: 212-905-0509
 8 Fax: 212-905-0508

E-filing

Filed

MAR 27 2012

RICHARD W. WIEKING
 CLERK, U.S. DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN JOSE

6 Martin S. Bakst (State Bar No. 65112)
 7 **LAW OFFICES OF MARTIN S. BAKST**
 8 15760 Ventura Boulevard, 16th Floor
 9 Encino, CA 91436
 10 Tel: 818-981-1400
 11 Fax: 818-981-5550

ADR

Attorneys for Plaintiff

11 **UNITED STATES DISTRICT COURT**
 12 **NORTHERN DISTRICT OF CALIFORNIA**

13
 14 MARIA PIROZZI, Individually and on Behalf
 15 of All Others Similarly Situated,

Plaintiff,

v.

APPLE INC.,

Defendant.

CV12-01529

HRL

CLASS ACTION COMPLAINT FOR

1. Unfair Competition, California Business and Professions Code § 1720
2. Violations of the Consumer Legal Remedies Act, California Civil Code § 1750
3. Unjust Enrichment
4. Negligent Misrepresentation

22 Plaintiff Maria Pirozzi, individually and on behalf of all others similarly situated, makes the
 23 following allegations based on her personal knowledge of her own acts and, otherwise, upon
 24 information and belief based on investigation of counsel.

NATURE OF THE ACTION

26 1. This is a class action brought on behalf of the Plaintiff and other owners and users
 27 of the Apple iPhone, iPod touch and/or iPad mobile devices (the "Apple Device") who purchased
 28

1 mobile software applications ("apps") from a website controlled by Apple, Inc. ("Apple" or the
2 "Company").

3 2. Plaintiff and other members of the proposed Class (as defined below) downloaded
4 apps to their Apple Device from an Apple-sponsored Website as part of the use of their mobile
5 devices. Apple claims to review each application before offering it to its users, purports to have
6 implemented apps privacy standards, and claims to have created a strong privacy protection for its
7 customers. However, unbeknownst to consumers such as Plaintiff, some of these apps have been
8 secretly uploading user personal information, including, but not limited to user names, contact list
9 (including names, addresses and phone numbers of users' contacts), photographs and videos
10 without user knowledge or consent. For example, users who allow apps to use location data,
11 which is used for GPS-based apps, are also unknowingly giving these apps access to the user's
12 private photo and video files that can be uploaded and saved on the app's servers.

13 3. Apple failed to properly safeguard Apple Devices and, instead, induced Plaintiff to
14 purchase an Apple Device and to download apps under the premise that Plaintiff's private
15 information would remain confidential and would not be shared with third-party developers
16 without Plaintiff's express consent.

17 4. Plaintiff did not consent to her private information being provided to third parties,
18 nor was she aware that these apps were able to do so. Plaintiff alleges that Apple invaded and/or
19 facilitated the invasion her privacy, misappropriated and misused her personal information, and
20 interfered with the operability of her mobile devices—conduct and consequences for which she
21 now seeks relief.

22 PARTIES

23 8. Plaintiff Maria Pirozzi is a citizen of New Jersey and is an owner of an Apple
24 Device. Plaintiff has owned an Apple Device since September 2011. During that time, she has
25 downloaded a number of apps from Apple's App Store.

26 5. Defendant Apple is a California corporation that is licensed to do, and is doing,
27 business in California and throughout the United States. Its principle place of business is in
28

1 Cupertino, California. The Company offers a range of mobile communication and media devices,
2 personal computing products, and portable digital music players, as well as a variety of related
3 software, services, peripherals, networking solutions and various third-party hardware and software
4 products. In addition, the Company offers its own software products, including iOS, the
5 Company's proprietary mobile operating system; server software; and application software for
6 consumer, education, and business customers. At all relevant times, Apple designed, manufactured,
7 promoted, marketed, distributed, and/or sold the iPhone, iPod Touch and iPad throughout the
8 United States and California. Apple also sold apps on its platform to be used by the Apple Devices.
9 Apple receives a portion of fees for apps that it sells in the App Store.

10 JURISDICTION AND VENUE

11 9. This Court has original jurisdiction of this action under the Class Action Fairness Act
12 of 2005. The amount-in-controversy exceeds the sum or value of \$5,000,000 exclusive of interest
13 and costs, and there is minimal diversity because certain members of the class are citizens of a
14 different state than any defendant as required by 28 U.S.C. § 1332(d)(2).

15 10. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant's
16 improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from
17 this judicial district.

18 CLASS ACTION ALLEGATIONS

19 11. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil
20 Procedure 23(a) and 23(b)(3) seeking injunctive relief on behalf of himself and all others similarly
21 situated as members of the following class (the "Class") consisting of all persons who purchased an
22 iPhone, iPod Touch or iPad between June 15, 2010 and the present.

23 12. Subject to additional information obtained through further investigation and
24 discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or
25 amended complaint. Specifically excluded from the proposed Class is Apple, its officers, directors,
26 agents, trustees, parents, children, corporations, trusts, representatives, employees, principals,
27 servants, partners, joint ventures, or entities controlled by Apple, and their heirs, successors,
28

1 assigns, or other persons or entities related to or affiliated with Apple and/or their officers and/or
2 directors, or any of them.

3 13. **Numerosity.** The members of the Class are so numerous that joinder of all members
4 is impracticable. Plaintiff is informed and believes, and on that basis alleges, that the proposed
5 Class currently contains well over two million members. The exact number of members of the
6 Class is unknown to Plaintiff at the present time. The true number of Class members are known by
7 Apple, however, and thus may be notified of the pendency of this action by first class mail,
8 electronic mail, and by published notice.

9 14. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and
10 protect the interests of the members of the Class. Plaintiff has retained counsel highly experienced
11 in complex consumer class action litigation and intends to prosecute this action vigorously.
12 Plaintiff is a member of the Class and does not have interests antagonistic to, or in conflict with, the
13 other members of the Class.

14 15. **Typicality.** Plaintiff's claims are typical of the claims of the members of the Class.
15 Plaintiff and all members of the Class purchased an Apple Device and have downloaded
16 applications on those devices and have sustained damages arising out of the same wrongful course
17 of conduct.

18 16. **Existence and Predominance of Common Questions of Law and Fact.** Common
19 questions of law and fact exist as to all members of the Class and predominate over any questions
20 solely affecting individual members. Among the questions of law and fact common to the Class
21 are:

22 a. Whether Apple violated: (i) California Business and Professions Code §
23 17200; (ii) The Consumer Legal Remedies Act, Cal. Civ. Code § 1750; and (iii) violations of
24 common law;

25 b. Whether Apple invaded and/or facilitated the invasion of privacy of the
26 Class;

27 c. Whether Apple was unjustly enriched thereby; and
28

1 d. Whether Apple made negligent misrepresentations to the Class.

2 17. **Superiority.** A class action is superior to other available methods for the fair and
3 efficient adjudication of this controversy since, among other things, joinder of all members of the
4 Class is impracticable. Furthermore, as the damages suffered by many individual Class members
5 may be relatively small, the expense and burden of individual litigation make it virtually impossible
6 for Class members individually to seek redress for the wrongful conduct alleged. Plaintiff does not
7 foresee any difficulty in the management of this litigation that would preclude its maintenance as a
8 class action.

9 18. The claims asserted herein are applicable to all individuals and entities throughout
10 the United States who purchased an Apple Device. The State of California has sufficient state
11 interest through a significant contact or aggregation of contacts to the claims asserted by each
12 member of the Class so that the choice of California law is not arbitrary or unfair.

13 19. Adequate notice can be given to Class members directly using information
14 maintained in Apple's records, or through notice by publication.

15 20. Damages may be calculated from the sales information maintained in Apple's
16 records, so that the costs of administering a recovery for the Class can be minimized. The amount
17 of damages is known with precision from Apple's records.

18 **SUBSTANTIVE ALLEGATIONS**

19 21. In July 2008, Apple launched the App Store where customers can shop for and
20 acquire apps offered by Apple and third-party developers. Currently, the App Store has over
21 500,000 third-party applications covering a wide variety of areas including games, news, health,
22 travel, education, business, sports, and social networking. According to Apple, the App Store and
23 the apps are integral to the iPhone:

24 Over 500,000 apps. For work, play, and everything in between. The apps that come
25 with you iPhone are just the beginning. Browse the App Store to find hundreds of
26 thousands more. The more apps you download, the more you realize there's almost
27 no limit to what your iPhone can do.
28

1 22. Apple makes similar claims regarding iPad and iPod Touch. With regards to the
2 iPad, Apple provides:

3 An app made for iPad is an app like no other. That's because apps for iPad are
4 designed specifically to take advantage of all the technology built into iPad. And
5 with over 200,000 apps to choose from, there's no telling where the next tap will
6 take you.

6 23. Apple has designed its iPhone, iPad and iPod Touch wireless mobile devices to
7 accept apps only from Apple's App Store, making Apple's App Store essentially the exclusive
8 source from which consumers may obtain apps for their Apple Devices.

9 24. Since July 2008, over 24 billion apps have been downloaded by customers using
10 Apple devices. In 2011 alone, Apple sold 72.3 million iPhone handsets and 32.4 million iPads.
11 Apple is reported to have captured 99.4% of the 4.5 billion sales of mobile apps in 2009 (with
12 associated gross App revenues of \$6.8 billion). Articles estimate that by 2013, total mobile app
13 revenues will reach a staggering \$29.5 billion. Apple's App Store had \$1.782 billion in revenues in
14 2010 and in excess of \$4 billion in revenues in 2011. While Apple shares app revenue with
15 developers, Apple nevertheless profits from the apps directly through sales and, more importantly,
16 through the increased popularity of its mobile devices.

17 25. In order to offer an application for download in the App Store, a third-party
18 developer must be registered as an "Apple Developer" and agree to the iOS Developer Agreement
19 (the "IDA") and the Program License Agreement (the "PLA") with Apple. Apple provides third-
20 party developers with review guidelines, and conducts a review of all applications submitted for
21 inclusion in the App Store for compliance with these documents. To get applications into the
22 AppStore, Apple requires developers to submit their App and wait for approval or rejection by
23 Apple (and rejected apps are given feedback on the reason they were rejected so they can be
24 modified and resubmitted).

25 26. The App Store Review Guidelines set forth the technical, design, and content
26 guidelines Apple will use when reviewing an app for inclusion in Apple's App Store. These
27 guidelines state that apps "cannot transmit data about a user without obtaining the user's prior
28

1 permission and providing the user with access to information about how and where the data will be
2 used.” This includes the transmission of personally identifiable information. In addition, the
3 requirements of the PLA empower users to control access to user or device data, and require user
4 consent before user or device data can be collected.

5 27. According to Apple, its operating system, iOS, “is highly secure from the moment
6 you turn on your iPhone. All apps run in a safe environment, so a website or app can’t access data
7 from other apps. iOS also supports encrypted network communication to protect your sensitive
8 information. To guard your privacy, apps requesting location information are required to get your
9 permission first. You can set a passcode lock to prevent unauthorized access to your device[.]”
10 Apple makes similar claims with respect to the iPad and the iPod Touch.

11 28. Indeed, according to the App Store’s development guidelines, “[t]he app approval
12 process is in place to ensure that applications are reliable, perform as expected, and are free of
13 explicit and offensive material. We review every app on the App Store based on a set of technical,
14 content, and design criteria.”

15 29. With respect to location-based services, the Apple privacy policy provides only that
16 the company may obtain anonymous location data that does not personally identify the user:

17 To provide location-based services on Apple products, Apple and our partners and
18 licensees may collect, use, and share precise location data, including the real-time
19 geographic location of your Apple computer or device. This location data is
20 collected anonymously in a form that does not personally identify you and is used
21 by Apple and our partners and licensees to provide and improve location-based
22 products and services. For example, we may share geographic location with
23 application providers when you opt in to their location services.

24 30. In contrast to Apple’s statements, Apple-approved apps have downloaded and/or
25 copy users’ private address book information (including names and contact information of users’
26 contacts), location data, private photographs and videos without the users’ knowledge or consent
27 when a user agrees to allow an app to access the user’s then current locations. These uses go well
28 beyond what a reasonable Apple Device user understands himself to be consenting to when she
allows an app to access data on the Apple Device for the app’s functionality.

1 31. For example, in early February 2012, it was uncovered that one such app, Path, was
2 uploading data stored on users' Apple Devices (including address book and calendar) to its servers,
3 causing the app developers' Chief Executive Officer to issue an apology to Path users:

4 **We are sorry**

5 We made a mistake. Over the last couple of days users brought to light an issue
6 concerning how we handle your personal information on Path, specifically the
7 transmission and storage of your phone contacts.

8 As our mission is to build the world's first personal network, a trusted place for you
9 to journal and share life with close friends and family, we take the storage and
10 transmission of your personal information very, very seriously.

11 Through the feedback we've received from all of you, we now understand that the
12 way we had designed our 'Add Friends' feature was wrong. We are deeply sorry if
13 you were uncomfortable with how our application used your phone contacts.

14 In the interest of complete transparency we want to clarify that the use of this
15 information is limited to improving the quality of friend suggestions when you use
16 the 'Add Friends' feature and to notify you when one of your contacts joins Path--
17 nothing else. We always transmit this and any other information you share on Path
18 to our servers over an encrypted connection. It is also stored securely on our servers
19 using industry standard firewall technology.

20 We believe you should have control when it comes to sharing your personal
21 information. We also believe that actions speak louder than words. So, as a clear
22 signal of our commitment to your privacy, we've deleted the entire collection of
23 user uploaded contact information from our servers. Your trust matters to us and we
24 want you to feel completely in control of your information on Path.

25 In Path 2.0.6, released to the App Store today, you are prompted to opt in or out of
26 sharing your phone's contacts with our servers in order to find your friends and
27 family on Path. If you accept and later decide you would like to revoke this access,
28 please send an email to service@path.com and we will promptly see to it that your
contact information is removed.

We care deeply about your privacy and about creating a trusted place for you to
share life with your close friends and family. As we continue to expand and grow
we will make some mistakes along the way. We commit to you that we will
continue to be transparent and always serve you, our users, first.

We hope this update clears up any confusion. You can find Path 2.0.6 in the App
Store [here](#).

Sincerely,
Dave Morin
Co-Founder and CEO

33. Indeed, copying address book data, photos and videos without a user's consent is against Apple's rules. Nevertheless, the Company failed to properly screen apps and allowed such apps to be sold in the App Store.

8 34. This significant data breach has led two members of Congress to write to Apple's
9 CEO to inquire about Apple's privacy problems:1

February 15, 2012

Mr. Tim Cook
Chief Executive Officer, Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
Dear Mr. Cook:

Last week, independent iOS app developer Arun Thampi blogged about her discovery that the social networking app “Path” was accessing and collecting the contents of her iPhone address book without ever having asked for her consent. The information taken without her permission – or that of the individual contacts who own that information – included full names, phone numbers, and email addresses. Following media coverage of Mr. Thampi’s discovery, Path’s Co-Founder and CEO Dave Morin quickly apologized, promised to delete from Path’s servers all data it had taken from its users’ address books, and announced the release of a new version of Path that would prompt users to opt in to sharing their address book contacts.

This incident raises questions about whether Apple's iOS app developer policies and practices may fall short when it comes to protecting the information of iPhone users and their contacts.

The data management section of your iOS developer website states: “iOS has a comprehensive collection of tools and frameworks for storing, accessing, and sharing data. . . . iOS apps even have access to a device’s global data such as contacts in the Address Book, and photos in the Photo Library.” The app store review guidelines section states: “We review every app on the App Store based on a set of technical, content, and design criteria. This review criteria is now available to you in the App Store Review Guidelines.” This same section indicates that the guidelines are available only to registered members of the iOS Developer Program. However, tech blogs following the Path controversy indicate that the iOS App Guidelines require apps to get a user’s permission before “transmit[ing] data about a user”.

Internal footnotes omitted.

In spite of this guidance, claims have been made that “there’s a quiet understanding among many iOS app developers that it is acceptable to send a user’s entire address book, without their permission, to remote servers and then store it for future reference. It’s common practice, and many companies likely have your address book stored in their database.” One blogger claims to have conducted a survey of developers of popular iOS apps and found that 13 of 15 had a “contacts database with millions of records” – with one claiming to have a database containing “Mark Zuckerberg’s cell phone number, Larry Ellison’s home phone number and Bill Gates’ cell phone number.”

The fact that the previous version of Path was able to gain approval for distribution through the Apple iTunes Store despite taking the contents of users’ address books without their permission suggests that there could be some truth to these claims.

* * *

35. Apple did not adequately respond to the Representatives’ letter, necessitating a March 14, 2012 follow-up:²

March 14, 2012

Mr. Tim Cook
Chief Executive Officer, Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Cook:

We have received and reviewed the reply of Apple Inc., to our February 15, 2012, letter requesting information about your company’s app developer policies and practices to protect the privacy and security of your mobile device users’ information. We thank you for responding to our letter.

The March 2 reply we received from Apple does not answer a number of the questions we raised about the company’s efforts to protect the privacy and security of its mobile device users. In addition, subsequent to our letter, concerns have been raised about the manner in which apps can access photographs on your mobile devices and tools provided by Apple to consumers to prevent unwanted online tracking. To help us understand these issues, we request that you make available representatives to brief our staff on the Energy and Commerce Committee.

* * *

36. On March 22, 2012, Representatives Waxman and Butterfield also sent letters to thirty-four sellers of apps inquiring about their information collection and use practices. These sellers included Foodspotting, Inc.; Synthetic, LLC (Disposable); Turntable.fm, Inc.; Twitter, Inc.;

² Internal footnotes omitted.

1 Foursquare Labs, Inc.; Quora, Inc.; Eye2i, Inc.(MusicPound); Tapbots, LLC (Tweetbot);
 2 Remixation (Showyou); Schematic Labs (Soundtracking); Massive Health, Inc.; Trover LLC;
 3 District Nerds, LLC; SoundCloud Ltd.; Hipster, Inc.; Forkley, Inc.; Tiny Review; Fashism, LLC;
 4 Path, Inc.; Banjo, Inc.; Redaranj, LLC (Recollect); Socialcam, Inc.; Brew Labs, Inc. (Pinterest);
 5 Piictu, Inc.; Stamped, Inc.; Burbn, Inc. (Instagram); Apple Inc., Glancee, Inc.; d3i Ltd. (Momento);
 6 LinkedIn Corporation; SK Plante, Co., Ltd. (dishPal); and Facebook. The following letter to Lucas
 7 Buick, CEO of Synthetic, LLC is an example of these letters:³

8 March 22, 2012

9 Mr. Lucas Buick
 10 Founder and Chief Executive Officer, Synthetic, LLC
 11 d/b/a Disposable
 74 Langton Street
 San Francisco, CA 94103
 Dear Mr. Buick:

12 Last month, a developer of applications ("apps") for Apple's mobile
 13 devices discovered that the social networking app Path was accessing and
 14 collecting the contents of his iPhone address book without having asked for his
 15 consent. Following the reports about Path, developers and members of the press
 16 ran their own small-scale tests of the code for other popular apps for Apple's mobile
 17 devices to determine which were accessing address book information. Around this
 time, three other apps released new versions to include a prompt asking for users'
 consent before accessing the address book. In addition, concerns were
 subsequently raised about the manner in which apps can access photographs on
 Apple's mobile devices.

18 * * *

19 37. Similar concerns were raised by Senator Charles E. Schumer who called for a
 20 Federal Trade Commission investigations into the "disturbing and potentially unfair practices in
 21 the smartphone application market":

22 FOR IMMEDIATE RELEASE: March 5, 2012

23 **SCHUMER CALLS FOR FTC INVESTIGATION OF APPLE AND**
 24 **ANDROID PHONE PLATFORMS THAT ALLOW APPS TO STEAL**
PRIVATE PHOTOS AND ADDRESS BOOKS AND POST THEM ONLINE –
 25 **WITHOUT CONSUMER'S CONSENT**

26 *Reports Over the Last Week Revealed That Applications Developed for iPhones*
 27 *and Android Operating Systems Allow Third Party Access to Information Like*
Address Books and Private User Photos, Without User's Permission

28 ³ Internal footnotes omitted.

Schumer Asks for Federal Trade Commission to Investigate and Determine if the Unauthorized Copying and Distribution of Private Information Stored on Cells Phones is an Unfair or Deceptive Practice

Schumer: When Someone Takes a Private Photo on their Private Phone, It Should be Just That: Private

United States Senator Charles E. Schumer today called for the Federal Trade Commission to launch an investigation into reports that smartphone applications sold on the Apple and Android platforms are allowed to steal private photos and customers address books. This past week, the New York Times revealed that iPhone and Android applications downloaded by users can actually gain access to a customer's private photo collection, and in some cases share the information online. This latest report comes on the heels of the discovery last month that applications on Apple devices like the iPhone and iPad were able to upload entire address books with names, phone numbers, and email address to their own servers. In both cases, users were not notified that their private information stored on their phone and or iPad could be copied and used by third party applications.

"When someone takes a private photo, on a private cell phone, it should remain just that: private," said Schumer. "Smartphone developers have an obligation to protect the private content of their users and not allow them to be veritable treasure troves of private, personal information that can then be uploaded and distributed without the consumer's consent."

According to reports by independent technologists, two separate loopholes, one in the Apple operating system and one in the Android operating system, allow apps to gather users' photos. In the case of Apple, if a user allows the application to use location data, which is used for GPS-based applications, they also allow access to the user's photo and video files that can be uploaded to outside servers. In the case of Android-based applications, the user only needs to allow the application to use Internet services as part of the app for third parties to gain access to photo albums.

"It sends shivers up the spine to think that one's personal photos, address book, and who-knows-what-else can be obtained and even posted online – without consent. If the technology exists to open the door to this kind of privacy invasion, then surely technology exists to close it, and that's exactly what must happen. The rapid innovation in technology, which is wonderful, must not also become an open invitation to violate people's privacy willy-nilly. When a consumer makes a private phone call or sends a letter the old fashioned way, they have a very reasonable expectation that the communication is private. The same standard must apply to our new technologies, too," continued Schumer.

Two weeks ago it was revealed that some of the most popular applications for smart phones were routinely collecting personal data from users' address books, despite policies in place from smartphone makers like Apple that explicitly prohibit such action without the prior consent of the user. After reports revealed this widespread practice, several applications announced they would end the practice. Questions remain, however, over the implementation of security policies employed by smartphone manufacturers and their oversight of applications sold on their platforms.

Schumer today, in a letter to the Federal Trade Commission, called for the agency to launch a comprehensive investigation to explicitly determine whether copying or

1 distributing personal information from smartphones, without a user's consent,
constitutes an unfair or deceptive trade practice. Schumer is also urging the agency

2 to require smart phone makers put in place safety measures to ensure third party
3 applications are not able to violate a user's personal privacy by stealing
photographs or data that the user did not consciously decide to make public.

4 38. The New York Times technology columnist Nick Bolton likewise called out Apple's
5 practices in a February 28, 2012 article entitled, *Apple Loophole Gives Developers Access to*
6 *Photos*:

7 SAN FRANCISCO — The private photos on your phone may not be as private as
8 you think.

9 Developers of applications for Apple's mobile devices, along with Apple itself,
came under scrutiny this month after reports that some apps were taking people's
10 address book information without their knowledge.

11 As it turns out, address books are not the only things up for grabs. Photos are also
vulnerable. After a user allows an application on an iPhone, iPad or iPod Touch to
12 have access to location information, the app can copy the user's entire photo
library, without any further notification or warning, according to app developers.

13 It is unclear whether any apps in Apple's App Store are illicitly copying user
14 photos. Although Apple's rules do not specifically forbid photo copying, Apple
says it screens all apps submitted to the store, a process that should catch nefarious
15 behavior on the part of developers. But copying address book data was against
Apple's rules, and the company approved many popular apps that collected that
16 information.

17 Apple did not respond to a request for comment.

18 The first time an application wants to use location data, for mapping or any other
purpose, Apple's devices ask the user for permission, noting in a pop-up message
19 that approval "allows access to location information in photos and videos." When
the devices save photo and video files, they typically include the coordinates of the
20 place they were taken — creating another potential risk.

21 "Conceivably, an app with access to location data could put together a history of
where the user has been based on photo location," said David E. Chen, co-founder
22 of Curio, a company that develops apps for iOS, Apple's mobile operating system.
"The location history, as well as your photos and videos, could be uploaded to a
23 server. Once the data is off of the iOS device, Apple has virtually no ability to
monitor or limit its use."

24 On Apple devices, full access to the photo library was first permitted in 2010 when
Apple released the fourth version of iOS. The change was intended to make photo

25 apps more efficient. Google declined to comment on how its Android operating
26 system for mobile devices handles this issue.

27 "It's very strange, because Apple is asking for location permission, but really what
28 it is doing is accessing your entire photo library," said John Casasanta, owner of the

1 successful iPhone app development studio Tap Tap Tap, which created the
2 Camera+ app. "The message the user is being presented with is very, very unclear."

3 The New York Times asked a developer, who asked not to be named because she
4 worked for a popular app maker and did not want to involve her employer, to create
5 a test application that collected photos and location information from an iPhone.
6 When the test app, PhotoSpy, was opened, it asked for access to location data. Once
7 this was granted, it began siphoning photos and their location data to a remote
8 server. (The app was not submitted to the App Store.)

9 The knowledge that this capability exists is not new, developers say, but it was
10 assumed that Apple would ensure that apps that inappropriately exploited it did not
11 make it into the App Store. Based on recent revelations, phone owners cannot be
12 sure.

13 "Apple has a tremendous responsibility as the gatekeeper to the App Store and the
14 apps people put on their phone to police the apps," said David Jacobs, a fellow at
15 the Electronic Privacy Information Center. "Apple and app makers should be
16 making sure people understand what they are consenting to. It is pretty obvious that
17 they aren't doing a good enough job of that."

18 "We've seen celebrities and famous people have pictures leaked and disclosed in
19 the past. There's every reason to think that if you make that easier to do, you'll see
20 much more of it," Mr. Jacobs said. Not just celebrities are at risk, she added. "A lot
21 of sites are trying to obtain images from everyday people and politicians to post
22 online."

23 As the Apple Store has grown to include more than 600,000 apps, and with Apple
24 facing pressure from Google and Android, some worry that the company is
25 becoming less vigilant about monitoring app developers, exposing users to
26 unnecessary risks and shoddy apps.

27 This month, Apple allowed a fake 99-cent Pokémon app into the App Store. Even
28 though it offered only a series of Pokémon images, it became one of the most
popular paid apps before it was removed by Apple.

39. Plaintiff considers her private data, including her address book information (including
names and contact information of users' contacts), location data, private photographs and videos to
be in the nature of confidential information and considers such information as personal property.

40. Apple failed to safeguard Plaintiff's personal information from potential
misappropriation.

41. Apple's conduct caused economic loss to Plaintiff in that her personal information
has discernible value, both to Apple and to Plaintiff. Likewise, Plaintiff and other members of the
Class have paid for apps sold through Apple's App Store that have left their private personal
information vulnerable to unauthorized access.

1 42. Plaintiff's experiences are typical of the experiences of Class Members.

2 **CLAIMS FOR RELIEF**

3 43. Based on the foregoing allegations, Plaintiff's claims for relief include the following:

4 **COUNT I**

5 **Violations of the Unfair Competition Law (UCL)**

6 **California Business and Professions Code, § 17200, *et seq.***

7 44. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

8 45. In violation of California Business and Professions Code, § 17200 *et seq.*, ("Unfair
9 Competition Law"). Apple's conduct in this regard is ongoing and includes, but is not limited to,
10 statements made by Apple and Apple's omissions, including as set forth above.

11 46. By engaging in the above-described acts and practices, Apple has committed an
12 unfair business practice within the meaning of the Unfair Competition Law and, as a result,
13 Consumers suffered substantial injury they could not reasonably have avoided other than by not
14 purchasing the product.

15 47. Apple's conduct lacks reasonable and legitimate justification in that Apple have
16 benefited from such conduct and practices while Plaintiff and the Class have been misled as to the
17 nature and integrity of Apple's products and services and have, in fact, suffered material
18 disadvantage regarding their interests in the privacy and confidentiality of their personal
19 information.

20 48. The acts and practices of Apple are an unlawful business act or practice because they
21 violate the laws identified in this Complaint, including Negligence, Breach of Express and Implied
22 Warranty of Merchantability, Fraud and Deceit, Negligent Misrepresentation, the Consumers Legal
23 Remedies Act, and California Business & Professions Code § 17500, as described below.

24 49. In addition, Apple's modus operandi constitutes a sharp practice in that Apple knew
25 and should have known that consumers care about the status of personal information and privacy
26 but are unlikely to be aware of and able to detect the means by which Apple and/or its licensors
27
28

1 were conducting themselves in a manner adverse to its commitments and its users' interests. Apple
2 is therefore in violation of the unfair prong of the Unfair Competition Law.

3 50. As discussed above, Plaintiffs and the members of the Class purchased Apple
4 products and apps directly from Apple and/or their authorized agents. Plaintiffs and members of
5 the Class were injured in fact and lost money or property as a result of such acts of unfair
6 competition.

7 51. Apple's acts and practices were fraudulent within the meaning of the Unfair
8 Competition Law because they were likely to mislead the members of the public to whom they
9 were directed.

10 52. Unless Defendant Apple is enjoined from continuing to engage in the unlawful,
11 unfair and fraudulent business acts and practices as described herein, Plaintiff and the Class will
12 continue to be injured by Apple's conduct.

13 53. The unlawful, unfair and fraudulent conduct described herein is ongoing and
14 continues to this date. Plaintiffs and the Class, therefore, are entitled to relief described below as
15 appropriate for this Cause of Action.

16 54. Plaintiff, on behalf of himself and on behalf of each member of the Class, seeks
17 restitution, injunctive relief, and other relief allowed under the Unfair Competition Law.

18 **COUNT II**

19 **Violations of False and Misleading Advertising Law (FAL)**

20 **California Business & Professions Code § 17500, *et seq.***

21 55. Plaintiffs incorporate by reference each and every preceding paragraph as though
22 fully set forth herein.

23 56. Apple's acts and practices as described herein have deceived and/or are likely to
24 deceive members of the Class and the public. Apple has repeatedly advertised that its products
25 were safe and secure. Apple has furthered assured consumers that it closely monitors the apps
26 available in the app store. Instead, Apple has left its customer vulnerable to unauthorized data
27 breaches.

59. In making and disseminating the statements alleged herein, Apple should have known its advertisements were untrue and misleading in violation of California Business & Professions Code § 17500, *et seq.* Plaintiffs and the Class members based their decisions to purchase the Apple Device and/or purchase apps through the App Store in substantial part on Apple's misrepresentations and omitted material facts. The revenues to Apple attributable to products sold in those false and misleading advertisements amount to millions of dollars. Plaintiff and the Class were injured in fact and lost money or property as a result.

61. As a result of Apple's wrongful conduct, Plaintiff and the Class request that this Court enjoin Apple from continuing to violate California Business & Professions Code § 17500, *et seq.* Such conduct is ongoing and continues to this date. Plaintiff and the Class are therefore entitled to the relief described below as appropriate for this Cause of Action.

**Violations of the Consumer Legal Remedies Act (CLRA),
California Civil Code, § 1750, *et seq.***

CLASS ACTION COMPLAINT

63. In violation of Civil Code, § 1750, *et seq.*, Apple has engaged and is engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiff, and such transactions are intended to and have resulted in sales of services to consumers.

64. Plaintiff and the Class Members are consumers as that term is used in the Consumer Legal Remedies Act because they sought or acquired Apple's good or services for personal, family, or household purposes. Apple's past and ongoing acts and practices include but are not limited to: Apple's representations that their services have characteristics, uses, and benefits they do not have, in violation of Civil Code, § 1770(a)(5).

65. Apple's representations that their services are of a particular standard, quality and grade but are of another standard quality and grade, in violation of Civil Code, § 1770(a)(7); and

66. Apple's advertisement of services with the intent not to sell those services as advertised, in violation of Civil Code, § 1770(a)(9).

67. Apple's violations of Civil Code, § 1770 have caused damage to Plaintiff and the other Class members and threaten additional injury if the violations continue. This damage includes the injuries and losses set forth above.

68. Under § 1782 of the CLRA, notice is not required as Plaintiff are seeking only injunctive relief.

69. Plaintiff will not serve this Complaint upon Apple until such time for Apple to respond to the letter has passed without an agreement to take the actions required by the CLRA on behalf of all affected consumers. Plaintiff and the Class are therefore entitled to all forms of relief requested below as provided under § 1780 of the CLRA.

70. Based on its knowledge or reckless disregard of the facts as detailed herein, Apple was guilty of acting with malice, oppression or fraud.

COUNT IV

Unjust Enrichment

71. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

6 74. Under principles of equity and good conscience, Apple should not be permitted to
7 retain the information and/or revenue that they acquired by virtue of their unlawful conduct. All
8 funds, revenue, and benefits received by Apple rightfully belong to Plaintiff and the Class, which
9 Apple has unjustly received as a result of their actions.

11 COUNT V

12 **Negligent Misrepresentation**

15 77. Apple claims to review each application before offering it to its users, purports to
16 have implemented app privacy standards, and claims to have created a strong privacy protection
17 for its customers.

79. At all times herein, Plaintiff and the Class were unaware of the falsity of Apple's statements. Plaintiff and the Class reasonably acted in response to the statements made by Apple when they purchased an Apple device and downloaded apps from the App Store.

27

28

DEMAND FOR RELIEF

A. WHEREFORE, Plaintiff, on behalf of herself and on behalf of the members of the Class defined herein, as applicable, pray for judgment and relief as follows as appropriate for the above causes of action:

B. An order certifying this case as a class action and appointing Plaintiff and her counsel to represent the Class;

C. A temporary, preliminary and/or permanent order for injunctive relief enjoining Apple from pursuing the policies, acts and practices complained of herein;

D. A temporary, preliminary and/or permanent order for injunctive relief requiring Apple to undertake an informational campaign to inform members of the general public as to the wrongfulness of Apple's practices; and

Dated: March 26, 2012

GARDY & NOTIS, LLP

By: 

Jennifer Sarnelli (242510)

James S. Notis

Kira German

560 Sylvan Avenue, Suite 3085

Englewood Cliffs, NJ 07632

Tel: 201-567-7377

Fax 201-567-7337

jsarnelli@gardylaw.com

Martin S. Bakst (State Bar No. 65112)

LAW OFFICES OF MARTIN S. BAKST

15760 Ventura Boulevard, 16th Floor

Encino, CA 91436

Tel: 818-981-1400

Fax: 818-981-5550

msb@mbakst.com

Attorneys for Plaintiff